Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
National Broadband Plan Recommendation To Create a Cybersecurity Roadmap	))	PS Docket No. 10-146
	)	
A National Broadband Plan for Our Future	)	GN Docket No. 09-51
	)	

To: The Commission

COMMENTS OF HARRIS CORPORATION

This filing is submitted on behalf of Harris Corporation ("Harris") before the Federal Communications Commission ("Commission") in response to the Commission's *Public Notice*[1] seeking comment on the creation of a Cybersecurity Roadmap, as recommended by the National Broadband Plan.[2] In particular, the Commission seeks comment identifying the most significant vulnerabilities to communications networks or end users and solutions to addressing such vulnerabilities, in coordination with federal partners. Through Harris' experience in the construction, management, and protection of broadband communications networks, Harris's Cyber Integrated Solutions Business Unit is in a highly qualified position to provide the Commission with input regarding the development of a Cybersecurity Roadmap. Some of the most significant cybersecurity vulnerabilities that should be addressed by the Commission's Cybersecurity Roadmap include (1) end user activity; (2) information technology ("IT") and

[1] In the Matter of the National Broadband Plan Recommendation to Create a Cybersecurity Roadmap, Public *Notice*, PS Docket No. 10-146 and GN Docket 09-51, DA 10-1354 (rel. Aug. 9, 2010) ("Cybersecurity Roadmap").

[2] Report to Congress, A National Broadband Plan for Our Future, Federal Communications Commission, p. 321 (Mar. 16, 2009).

information assurance ("IA") workforce skill sets; and (3) deficient enterprise IT continuous monitoring and oversight. Harris believes increased education, training, and implementation of enhanced and continuous trusted monitoring techniques will help address the aforementioned cybersecurity vulnerabilities. Working in conjunction with industry, academia and government partners (domestic and when appropriate international) will be vital in addressing the cybersecurity network vulnerabilities identified by the Commission and included in the Commission's Cybersecurity Roadmap.

I. Harris Has An Extensive Background in Network Construction, Management, and Security and Is in the Process of Establishing the Nation's First Cyber Integration Center.

Harris is an international communications and information technology company, headquartered in Melbourne, Florida, that serves government and commercial markets in more than 150 countries. For decades Harris has used state-of-the-art technology assessment techniques and architecture engineering design methods to define, deliver, operate, and secure communications networks. Harris technology, countermeasures, and monitoring capabilities have effectively safeguarded vital information systems that support the critical missions of military, intelligence, and local and federal law enforcement customers. Harris operates some of our nation's largest and most secure, mission-critical networks.

For example, since 2002 Harris has performed as the prime contractor on the 15-year Federal Aviation Administration ("FAA") Federal Telecommunications Infrastructure ("FTI") program to integrate and modernize the U.S. air traffic control system and infrastructure. FTI is a modern, secure, and efficient network that provides secure voice, data, and radar communications to more than 4,000 FAA and Department of Defense sites across the country (including Alaska, Hawaii, and Puerto Rico). The FTI program has helped to reduce overall

FAA operating costs while enhancing network efficiency, reliability, security, and service. In February 2008 Harris successfully completed the transition of FAA legacy networks to the new FTI network. Harris now also operates the FAA's 24x7 Security Operations Center that monitors and mitigates FACC Wide Area Network vulnerabilities and threats.

Harris is utilizing its understanding of communications networks and applications to develop innovative solutions to ensure security and reliability across broadband networks in the government and a wide range of private industries. One such innovative solution is Harris' plan to build the nation's first Cyber Integration Center, which will provide government and commercial customers with a unique secure managed hosting service in a trusted computing environment. The Harris Cyber Integration Center will provide customers with an innovative on-demand integrated offering of infrastructure, managed security, tailored hosting and services—all provided as a secure, trusted total solution.

II. Key Cybersecurity Vulnerabilities that Should be Addressed By the Commission's Cybersecurity Roadmap Include End User Activity, IT and IA Workforce Skill Sets, and Enterprise IT Infrastructure Monitoring and Oversight.

As has been noted by the Commission, "cybersecurity is a vital topic for the Commission because end user lack of trust in online experiences will quell demand for broadband services and unchecked vulnerabilities in the communications infrastructure could threaten life, safety and privacy."[3] The purpose of the Commission's Cybersecurity Roadmap is to identify vulnerabilities before they inflict havoc the nation's broadband infrastructure. Three main cybersecurity vulnerabilities that should be addressed by the Commission in its Cybersecurity Roadmap are (1) end user activity; (2) IT and IA workforce skill sets, and (3) deficient enterprise IT infrastructure continuous monitoring and oversight. While there may be other more minute

[3] Cybersecurity Roadmap, *supra* note 1, p. 1.

vulnerability concerns, it is vital that the Commission addresses these core issues if the Commission wants to ensure the nation's broadband infrastructure is secure from cyber attack.

Many end users are unfamiliar with security policies, do not understand why policies and practices must be followed, and are generally uneducated about basic cybersecurity best practices. As a result, malicious code, often without the knowledge of the end user, is easily inserted into the nation's private and public information technology environment. A lack of user education consists both of a lack of knowledge of security protocols and a lack of understanding as to why on-line security protocols are necessary. In fact, with the nation's growing reliance on e-mail and social media networks are becoming even more vulnerable to phishing and other cybersecurity attacks resulting in easy access into secured networks and the data within. These malicious activities have a significant monetary impact. Estimates of U.S. industry economic losses resulting from data theft that caused loss of intellectual property are as high a one trillion dollars.[4] Network access through end users is one of the biggest network vulnerabilities to secure data networks throughout the nation's broadband infrastructure.

In order to promote a secure broadband infrastructure the nation's IT and IA workforce must develop critical cybersecurity skill sets to address key network vulnerabilities. Today, many technical controls are insufficient to prevent a full range of cyber attacks. Technical controls are often outdated, while threat actors, such as hackers, employ sophisticated and targeted attacks that exploit any vulnerability in hardware and software security. It is crucial that software patches are uploaded to systems in a timely manner and that IT enterprise managers have a keen awareness of trusted computing methods in both hardware and software. To

[4] McAfee, Inc. Research Shows Global Recession Increasing Risks to Intellectual Property, Press Release (Jan. 2009) available at www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html. *See also* McAfee, "Unsecured Economies: Protecting Vital Information" (Jan. 2009) available at http://resources.mcafee.com/content/NAUnsecuredEconomiesReport.

promote IT and IA workforce core and cutting edge competency the Commission should encourage members of the IT and IA workforce to remain educated on emerging security threats, vulnerabilities, and the available mitigation methods on a near real time basis. In furtherance of this goal, the Commission should encourage industry, government, and academia to establish incentives for those employees to be trained, and where warranted and feasible, to promote economic and honorary incentives (*i.e.,* training certifications) to ensure the confidentiality, integrity, and availability of critical network infrastructures.

Currently within many enterprises' IT infrastructure there is insufficient supply chain integrity, both on the software and hardware level, and a lack of continuous network oversight. These deficiencies represent a significant gap in enterprises' information technology infrastructure security. The resulting flawed situational awareness inhibits the enterprise from preventing new threats and vulnerabilities from endangering critical networks, and implementing appropriate cybersecurity vulnerability mitigation plans. In addition, in many enterprises' IT infrastructure, security is bolted on, not imbedded. Legacy enterprise IT infrastructure systems were built primarily with ease of use as a primary concern and security as a secondary thought. The Commission, through its Cybersecurity Roadmap, should encourage additional network monitoring and oversight on a continuous basis through enhanced software and hardware monitoring that can be used to identify changes in configuration and data integrity. For example, encouraging the implementation of solutions that deliver automated and updated threat, risk, and vulnerability feeds will greatly increase enterprise IT infrastructure security. New continuous security monitoring conducted either internally or through third party vendors can improve the security posture of enterprise IT systems.

III. The Commission Should Coordinate Its Cybersecurity Efforts With Industry, Academia, and Other Government Partners.

The Commission can ensure that effective security controls are in place within the nation's broadband infrastructure by cultivating its working relationships with industry, standard setting organizations, academia, and government, such as the Department of Homeland Security, National Institute of Science and Technology, the Network Reliability and Interoperability Council, and the American National Standards Institute. In order to ensure Commission initiatives do not contradict or mitigate other ongoing cybersecurity efforts, the Commission must take into consideration the efforts of other government entities (domestic and where appropriate international), as well as private industry, before taking action. As Harris pointed out in its Reply Comments concerning the Commission's proposed Cyber Certification Program, "the Commission may be better served at this time by continuing to emphasize compliance with standard setting bodies, conducting periodic reviews of the state of the cyber security industry, interfacing with other government entities to create uniform standards, and taking steps to promote a culture of diligent and informed cyber security practices amongst consumers."[5]

A number of efforts should be encouraged by the Commission in its Cybersecurity Roadmap to increase mitigation efforts and help ensure the confidentiality, integrity, authentication, and availability of communications networks and user data, such as:

- Widespread adoption of trusted computing technologies, such as the use of Trusted Platform Modules, already imbedded in over three million computers, and Root of Trust for Measurement (RTM), along with supply chain anchored hardware and software provenance and attestation.
- Engagement with industry, academia, and government bodies (domestic and when appropriate international) in crafting and defining policies.
- Ongoing development of cybersecurity "communities of interest."

[5] Comments of Harris Corporation, In the Matter of Cyber Security Certification Program, PS Docket No. 10-93, p. 8 (filed Sept. 8, 2010).

- Implementing rapid non-attributable reporting methods by stakeholders of new and existing vulnerabilities.
- Continuous monitoring in real time, as opposed to periodic reporting.
- Internal auditing and reporting of information technology environment scans, breaches, and actions.
- Use of existing information assurance programs and new third party vendor offerings to oversee, monitor, and confirm the use of appropriate cybersecurity protocols, both preventative and reactive.

As previously noted by Harris, "Commission participation in interagency organizations, such as the National Communications System's Information Sharing and Analysis Center, will allow the Commission to ensure that the telecommunications industry's cybersecurity concerns are taken into account in other governmental entities actions and that equity between private and public broadband cybersecurity is increased."[6] In particular, the Commission should:

- Work with its federal partners to encourage mid level and senior government IT security subject matter experts to engage with subject matter experts across industry to discuss how to address cybersecurity vulnerabilities.
- Coordinate with other government partners on what role the Commission is best suited to perform within existing efforts.
- Facilitate an understanding among stakeholders of existing domestic and international laws, agency and executive directives, and other notable government and industry policies.

IV. Conclusion

Harris respectfully submits these comments for the consideration of the Commission. Some of the most significant cybersecurity vulnerabilities that should be addressed in the Commission's Cybersecurity Roadmap include (1) end user activity; (2) IT and IA workforce cybersecurity skill sets; and (3) deficient enterprise IT infrastructure continuous monitoring and oversight. The vulnerabilities identified by Harris in these Comments warrant the Commission's attention and if addressed will advance the implementation of trusted computing technologies. When implementing its Cybersecurity Roadmap, the Commission must coordinate with industry,

[6] Comments of Harris Corporation, In the Matter of Effects on Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload, PS Docket No. 10-92, p. 6 (filed Sept. 3, 2010).

academia, and government entities (domestic and when appropriate international) to prevent acting in contradiction with existing industry and government efforts. Harris stands ready to work with both the public and private sector to provide innovative solutions, such as Harris' Cyber Integration Center, in order implement trusted computing technologies and effectively secure both cyberspace and the nation's broadband infrastructure.

Respectfully submitted,

HARRIS CORPORATION
600 Maryland Avenue, S.W.
Suite 850E
Washington, D.C. 20024
(202) 729-3700

_______/s/__________________________

Carl M. Bradley
Sales Engineer, Cyber Integrated Solutions

Evan S. Morris, Esq.
Legal Analyst, Government Relations

September 23, 2010